Efficient Authentication Protocols for Mobile Hand-held Devices with Minimum Power Consumption

K. Sathish Kumar[1], R. Sukumar[2], S. Kharthikeyan[3]

[1]*Assistant Professor, Department of Information Technology, Sethu Institute of Technology, Kariapatti, TamilNadu, India*
[2]*Professor, Department of Information Technology, Sethu Institute of Technology, Kariapatti, TamilNadu, India*
[3]*Post Graduate M.E Student, Department of Computer Science and Engineering, Sethu Institute of Technology, Kariapatti, TamilNadu, India.*

Abstract*: Mobile phone in day-to-day life has become an important communication device, subjected from formal and informal talks to sharing important and secure information. These secure information falls from personal communication to large business deals. Hence, there is a necessity to ensure security to the applications that are used to transfer confidential information. In order to satisfy the users' requirement, many cryptographic protocols are chosen based on confidentiality, integrity and performance. Public Key Cryptography is one such solution that meets the above mentioned attributes. Systems that use public key cryptography weigh computing power, key size to measure the efficiency of the protocol. This paper mainly focuses on the performance attributes of the various public key cryptography algorithms. Here, the algorithms RSA and ECC are studied and compared. These algorithms implemented, provide the necessary basic security components like confidentiality, authentication, integration and non-repudiation of services for a mobile communication. In addition to the performance characteristics of the algorithms studied, we also extend our research in analyzing the power consumed by these efficient cryptographic protocols. The protocols' energy efficiencies are measured based on the consumption of current, power against time.*

Keywords*: ECC, Energy Profiler, NTRU, Public Key Cryptography, RSA*

I. Introduction

In day to day life, from personal work to business sectors, mobile phones have become an essential communication device for the mankind. Recently, mobile phones are not only used for casual greetings but also, sending and receiving important data such as, social security numbers, bank account details and passwords etc. Thus, we need some cryptographic algorithms to ensure protection of such secured and confidential data on the mobile devices.

Any application in a mobile device consume significant amount of energy in order to perform. And the cryptographic algorithms that are used in mobile devices for transferring secured data are no longer an exception that consumes a high power from the battery. The problem in any mobile device is that its limited battery capacity. Today, the world is moving at a great pace in mobile device technology, in terms of smartphone. Such phones have a very limited battery capacity. Therefore, any application that is supposed to perform on mobile phones has a very less battery power for consuming the energy.

The battery capacity of handheld devices grows up only about 5% to 10% every year, which is insufficient for the electricity that the devices demand. High complexity of operations consumes significant amounts of energy, which becomes a challenge for battery-powered handheld devices.

The above discussed problems motivated to research and analyze and later work on the above issues. This work is focused to select the correct cryptographic algorithms to send a data in a secured and confidential manner. In order to do so, energy efficient authentication protocols are proposed for mobile hand-held devices. These protocols are developed to resolve the power consumption issue in a mobile device while performing cryptographic operations.

These cryptographic protocols which are energy efficient are designed to achieve uncompromised authenticate security systems. This means the protocols provide the key features of information security like confidentiality, integrity and authentication without any compromise to external factors that try to break the security. Hence, the proposed cryptographic protocol will provide a better security guarantee and acquires much less energy consumption than the existing cryptographic protocols.

II. Preliminaries And Related Works

Prior work on authentication protocols focused to find out a suitable protocol like NTRU for mobile communications [1] that are efficient than other conventional algorithms like RSA and ECC. The authors ([3], [11]) have studied the performance comparison for variable sized images and files as input. Though the encryption and decryption are high in NTRU, the RSA algorithm provides highest security to the business application. Efficient function called point multiplication has been discussed [5] to improve the performance of elliptic curve cryptography. The energy consumption of the proposed protocol for mobile handheld devices is considered as the basis for future work. Also, articles proposed ([6], [10]) is a base for calculating any cryptographic protocol's efficiency and strength.

With the recent changes in mobile technology, our work includes a thorough background study on the power consumption of the hand-held mobile devices in various scenarios. In case of Android mobile operating systems, the energy consumption is measured [2] using PowerTutor application which provides total power consumed by all the components and also displays remaining power in the battery of the mobile handheld device. The researchers have also analyzed ([4], [9]) the study of power consumption for data transfer by developing a simple Android application when using Bluetooth, 3G, GSM and WiFi. Similar analysis [6] like comparison cost drawn between energy, throughput, energy performance, average energy consumption of various algorithms like RSA, ECC, battery discharge of a component in each state [7], power for idleness of the system and during data transmission [8], power exhausted [12] and impact of a battery life while using the protocols [13] are also taken into consideration in this work.

III. Public Key Cryptographic Algorithms

In this section, we discuss the operations of algorithms RSA and ECC

3.1 RSA ALGORITHM

RSA is an algorithm for public key encryption that works out for signing as well as for encrypting. Known as one of the great advances in public key cryptography, RSA is used in day-to-day e-commerce protocols and is considered to be secure for modern application implementations.

3.1.1 RSA KEY GENERATION

RSA involves a public key and a private key. The public key is known to everyone and is used in encrypting the message. Those messages encrypted with the public key can be decrypted only with the private key. Two prime numbers p and q are chosen such that both are of equal bit length.

- n is computed such that $n=p*q$
- φ (n) computed such that $\varphi (n) = (p-1)* (q-1)$
- Select a random number e, such that, $e < \varphi (n)$ and $\gcd (e, \varphi (n)) =1$
- Compute integer d, such that $e*d = 1 \bmod \varphi (n)$
- Public key is (n,e) and d is the private key

3.1.2 RSA ENCRYPTION

Sender A transmits public key (n,e) to receiver B and keeps the private key secret. B then sends a message M to A. B turns M into a number such as $m < n$ by a padding scheme. The corresponding cipher text c is computed as follows:

$$c = m^e \bmod n_c$$

The cipher text is computed the method of exponentiation by squaring. B then sends cipher text c to A.

3.1.3 RSA DECRYPTION

A recovers m from cipher text c using its private key d in the following process:

$$m=c^d \bmod n$$

Given m, A can retrieve the original message M by the following computation:

$$c^d = (m^e)^d = m^{ed} \pmod n$$

3.2 ECC ALGORITHM

Elliptic curve cryptography (ECC) is a public key cryptography approach based on algebraic structure of elliptic curves over finite fields. Such elliptic curves are used for factorization algorithms in cryptographic applications.

An elliptic curve is a plane curve defined by a cubic equation of the form:

$$y^2 = x^3 + ax + b,$$

where a and b are real numbers.

3.2.1 ECC ALGORITHM STEPS

Step 1: A curve in the form of $y^2 = x^3 + ax + b$ is taken where a and b are curve parameters.

Step 2: Choose a prime number

Step 3: To compute the points on the elliptic curve, use point adding and point doubling.

Step 4: A generating point out of those points is chosen which is of large order.
Step 5: Select a random number which is less than the order of generating point. This serves as private key for each entity.
Step 6: Multiply the generating number with the secret number to get the public key.

3.2.2 ECC ENCRYPTION PROCESS

The plaintext message M is embedded into a point P_M from the finite set of points in elliptic group, E_p (a,b). A generator point, G € E_p(a,b) is chosen such that smallest value of n for which nG=O is a very large prime number. The elliptic group, E_p (a,b) and the generator point G are made public.

Select a private key, $n_A < n$ and compute public key $P_A=n_AG$. To encrypt the message point P_M for receiver, sender chooses a random integer *k* and computes the cipher text pair of points P_c using receiver's public key P_B

$$P_c = [\ kG, (\ P_M + kP_B)\ ]$$

3.2.2 ECC DECRYPTION PROCESS

After receiving the pair of cipher text points, P_c, the first point *k*G is multiplied with the receiver's private key n_B and then the result is added to the second point in the cipher text pair of points, ($P_M + kP_B$)

$$(P_M + kP_B) - [n_B(kG)] = (P_M + kn_BG) - [n_B(kG)] = P_M\,,$$

which is the plain text point, corresponding to the plaintext message M. Only the receiver, knowing the private key, n_B, can remove $n_B(kG)$ from the second point of the cipher text pair of point, i.e. ($P_M + kP_B$), and hence retrieve the plain text information P_M

IV. Experimental Evaluations

In this section we describe results from empirical measurements on a mobile device

4.1 Methodology:

The results shown in this section are based on the Nokia S60 edition device which runs in Symbian operating system. Power consumption was measured using the Nokia Energy Profiler Version 1.2. This application provides power consumption, as well as battery voltage and current, cumulative energy consumption, processor activity, RAM use, IP-network speeds, mobile-network signal strengths, 3G timers and WLAN signal strength. For our work, when we use the protocol, the Nokia Energy Profiler can be run in the background to profile power consumption. To enable easy identification of power-consumption events, the Nokia Energy Profiler can capture screen shots as part of the profile data. Fig 1 shows the methodology deployed in the mobile device to calculate the power and current consumption while using the protocols.

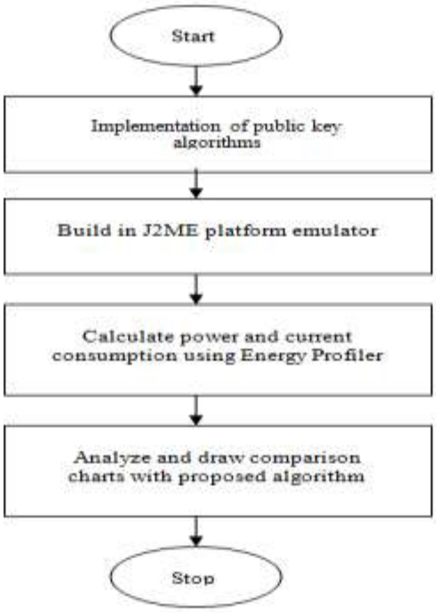

Start
Implementation of public key algorithms
Build in J2ME platform emulator
Calculate power and current consumption using Energy Profiler
Analyze and draw comparison charts with proposed algorithm
Stop

Fig.4.1 Methodology

4.2 Power and Current View

Power view (Fig 2) shows power consumption over a period when the protocols are used in the mobile device. The basic unit is a watt (W). Current view (Fig 3) displays current consumption, which is the measured current drawn from the battery.

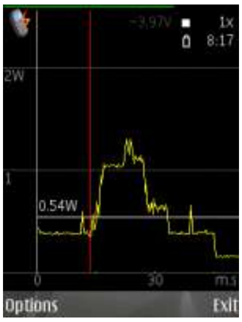


Fig.4.2.1 Power View

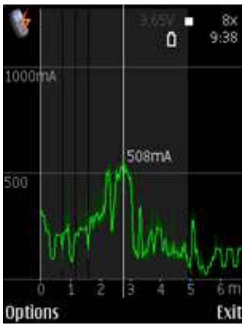
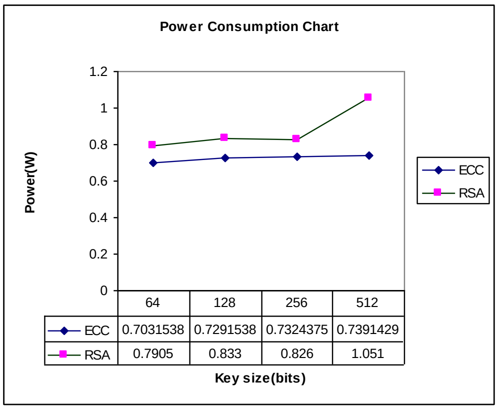


Fig.4.2.2 Current View

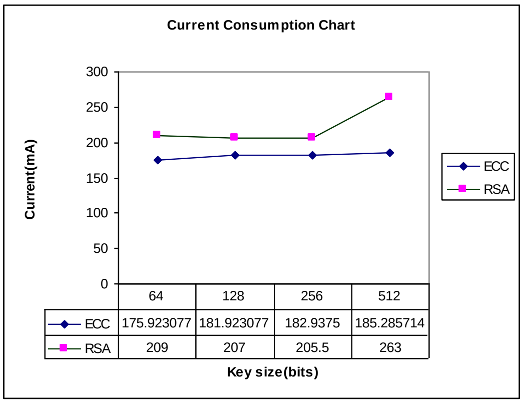
4.3 Results:

Following statistics are noted after evaluating the performance of the cryptographic protocols RSA and ECC in Nokia S60 device. The comparison charts are shown for power and current consumption of the RSA and ECC protocols in a mobile device for various key sizes..



	64	128	256	512
ECC	0.7031538	0.7291538	0.7324375	0.7391429
RSA	0.7905	0.833	0.826	1.051

Fig. 4.3.1 Power consumption on key sizes



	64	128	256	512
ECC	175.923077	181.923077	182.9375	185.285714
RSA	209	207	205.5	263

Fig.4.3 2 Current consumption on key sizes

V. Conclusions

In this work, a framework is presented for analyzing the energy consumption of conventional cryptographic algorithms. From the implementation of RSA and ECC algorithms, we now can conclude that in RSA, key generation and encryption are faster whereas decryption is slower. On the other hand, in ECC key generation and encryption are slower whereas the decryption is faster. The study shows ECC is power and energy efficient than RSA in mobile devices. Performance analysis shows the comparison of the existing cryptographic protocols. Hope this work to be a big contribution to the development and widespread acceptance of mobile commerce applications. So, as part of the future enhancement on this work, the NTRU algorithm with its change in encryption and decryption parameters, will be analyzed and compared with these implemented algorithms.

REFERENCES

[1] Sameer Hasan Al-Bakri, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan and Gazi Mahabubul Alam, "*Securing peer-to-peer mobile communications using public key cryptography: New security strategy*", *International Journal of the Physical Sciences Vol. 6(4)*, pp. 930-938, 18 February, 2011

[2] Vinod Namboodiri, Toolika Ghose, "*To Cloud or Not To Cloud – A Mobile Device Perspective on Energy Consumption of Applications*", *IEEE World of Wireless, Mobile and Multimedia Networks*, pp. 1-9, 25-28 June, 2012

[3] A. Naresh Reddy,Rakesh Nayak,S. Baboo,"*Analysis and Performance Characteristics of Cryptosystem using Image Files*",*International Journal of Computer Applications (0975 – 8887) Volume 51– No.22*, August 2012

[4] Goran Kalic, Iva Bojic and Mario Kusek, "*Energy Consumption in Android Phones when using Wireless Communication Technologies*", *MIPRO, 2012 Proceedings of the 35th International Convention*, 21-25 May 2012

[5] K. Sathish Kumar,R. Sukumar, P. Asrin Banu, "*An Experimental Study on Energy Consumption of Cryptographic Algorithms for Mobile Hand-Held Devices*", *International Journal of Computer Applications (0975 – 8887) Volume 40– No.1*, February 2012

[6] Helena Rif`a-Pous and Jordi Herrera-Joancomart, "*Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices*", *Future Internet 2011*, 3, 31-48, Published: 14 February 2011

[7] Lide Zhang, Birjodh Tiwana, Zhiyun Qian, Zhaoguang Wang, Robert P. Dick, Z. Morley Mao, Lei Yang, "*Accurate Online Power Estimation and Automatic Battery Behavior Based Power Model Generation for Smartphones", IEEE Hardware/Software Codesign and System Synthesis*, Pages 105-114, 24-29 October, 2010

[8] Andrew Rice and Simon Hay, "*Measuring mobile phone energy consumption for 802.11 wireless networking", Elsevier*, July 18, 2010

[9] Niranjan Balasubramanian,Aruna Balasubramanian,Arun Venkataramani, "*Energy Consumption in Mobile Phones: A Measurement Study and Implications for Network Applications" Association for Computing Machinery*, November 4–6, 2009, Chicago, Illinois, USA

[10] Vivek B. Kute, P. R. Paradhi and G. R. Bamnote, "*A software comparison of RSA and ECC", International Journal Of Computer Science And Applications Vol. 2, No. 1*, April / May 2009

[11] Challa Narasimham, Jayaram Pradhan, "*EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYSTEM USING TEXT FILES", Journal of Theoretical and Applied Information Technology, Vol. 4 No. 1*, 31st Jan 2008

[12] Niu Limin, Tan Xiaobin, Yin Baoqun, "*Estimation of System Power Consumption on Mobile Computing Devices", International Conference on Computational Intelligence and Security 2007*

[13] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan and Niraj K. Jha,"*A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 2*, FEBRUARY 2006

[14] Jha, R., Saini, A.K." *Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement", International conference on Communication Systems and Network Technologies (CSNT)*, 3-5 June 2011

[15] Wander, A.S.; Gura, N.; Eberle, H.; Gupta, V.; Shantz, S.," *Energy analysis of public-key cryptography on small wireless devices", IEEE TRANSACTIONS ON Pervasive Computing and Communications*, MARCH 2005